Boosting Cyber Resilience - Black Swans, Gray Rhinos and Coordinated Response

Beth Dunphy
Director, CISO and Privacy Leader
IBM Security

October 2020

IBM Security

Agenda

The Menagerie of Crisis

Preparing for Success

Evaluate and Continually Improve

Building a Cyber Resilient organization

90%

Of small businesses will fail in under a year in a disaster

26%

Of organizations have an enterprise-wide Incident Response Plan

$11,600

Per minute cost of an IT Outage for a large enterprise

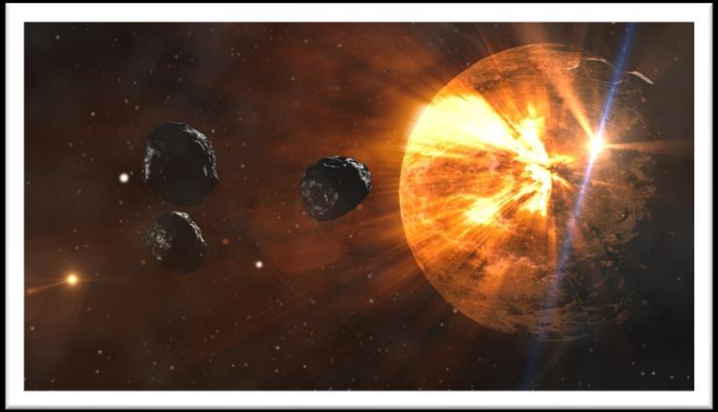
54%

Organizations report having downtime lasting over 8 hours in a single event

”By uncertain knowledge, let me explain… About these matters there is no scientific basis on which to form any calculable probability.”

- John Maynard Keynes

Royalty-free image by PickPik



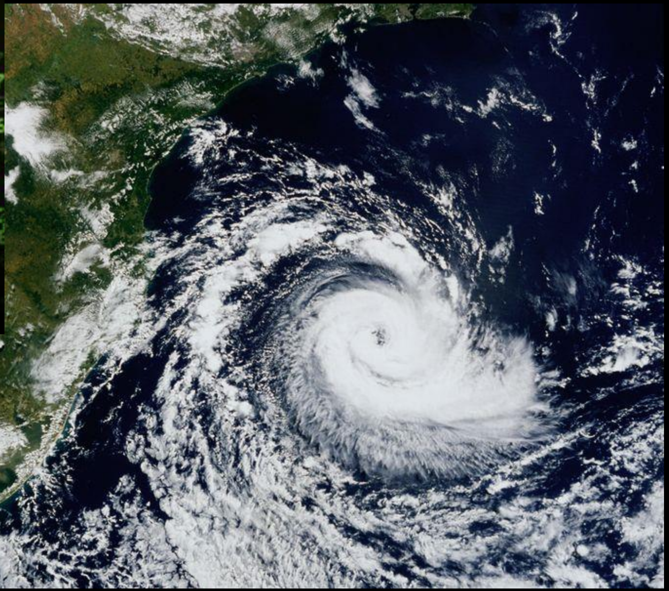
Black Swans are the inspiration for movies, literature and crisis planning

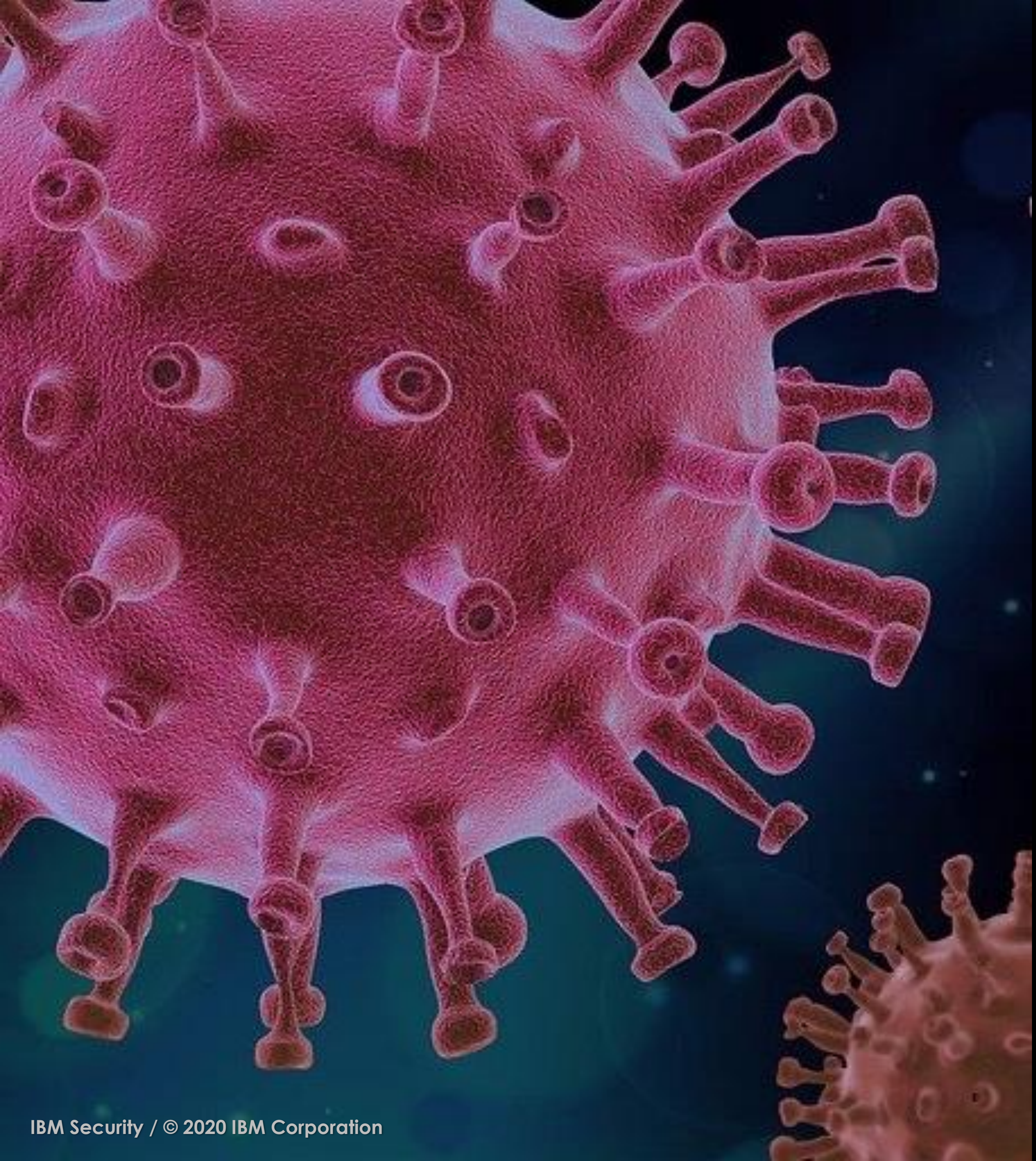
Spotting Gray Rhinos

"In any moment of decision, the best thing you can do is the right thing, the next best is the wrong thing, and the worst thing you can do is nothing."

- Theodore Roosevelt

Behind every Black Swan is a crash of Gray Rhinos





Is Covid-19 a Black Swan or a Gray Rhino?

Warning… Crisis is closer than it appears

Image Source: Pixabay

Listen to the Cassandras in your organization

Cassandras among us

- Technical Experts
- Data Driven
- Questioners

Preparing for success during crisis

Create your ”Dream Team”

One team with
One goal

Plan and Automate

Reduce complexity and increase integration

Prepare Communications

Clear, concise, targeted and timely

Test your plan and Measure Success

Test multiple scenarios using different methods

Measure and Report

Creating your own "Dream Team"

- ✓ Business Leaders
- ✓ Technical Leaders
- ✓ Cybersecurity
- ✓ Privacy
- ✓ Human Resources
- ✓ Marketing / Communications
- ✓ Legal
- ✓ Key Suppliers

Business Continuity + Incident Response + Privacy = Success!!

Plan your work and work your plan

Create an enterprise-wide plan for

- Business Continuity
- Disaster Recovery
- Incident Response

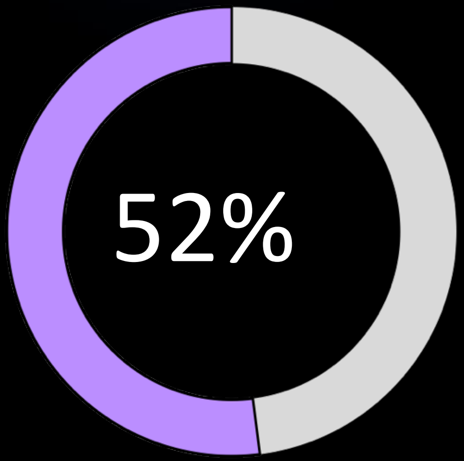
Consider regional or site level plans based on your organization

Tailor plans to address the unique characteristics of the organization

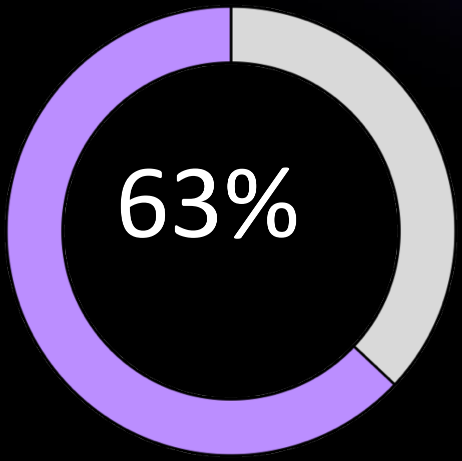
- Industry
- Geography
- Technology stack

Develop Playbooks to cover specific crisis scenarios

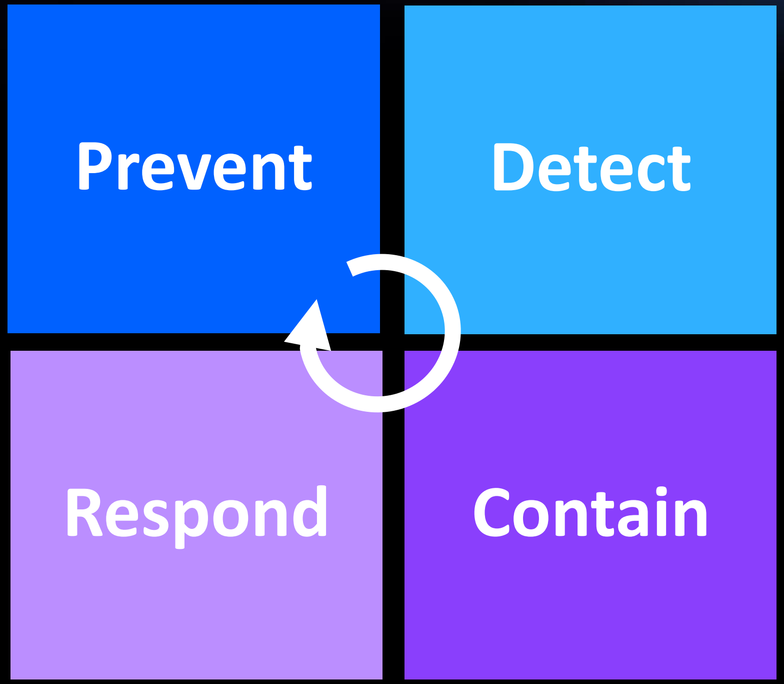
Automate to reduce complexity and increase resiliency



Ratio of respondents who say that Cloud services improved cyber resilience

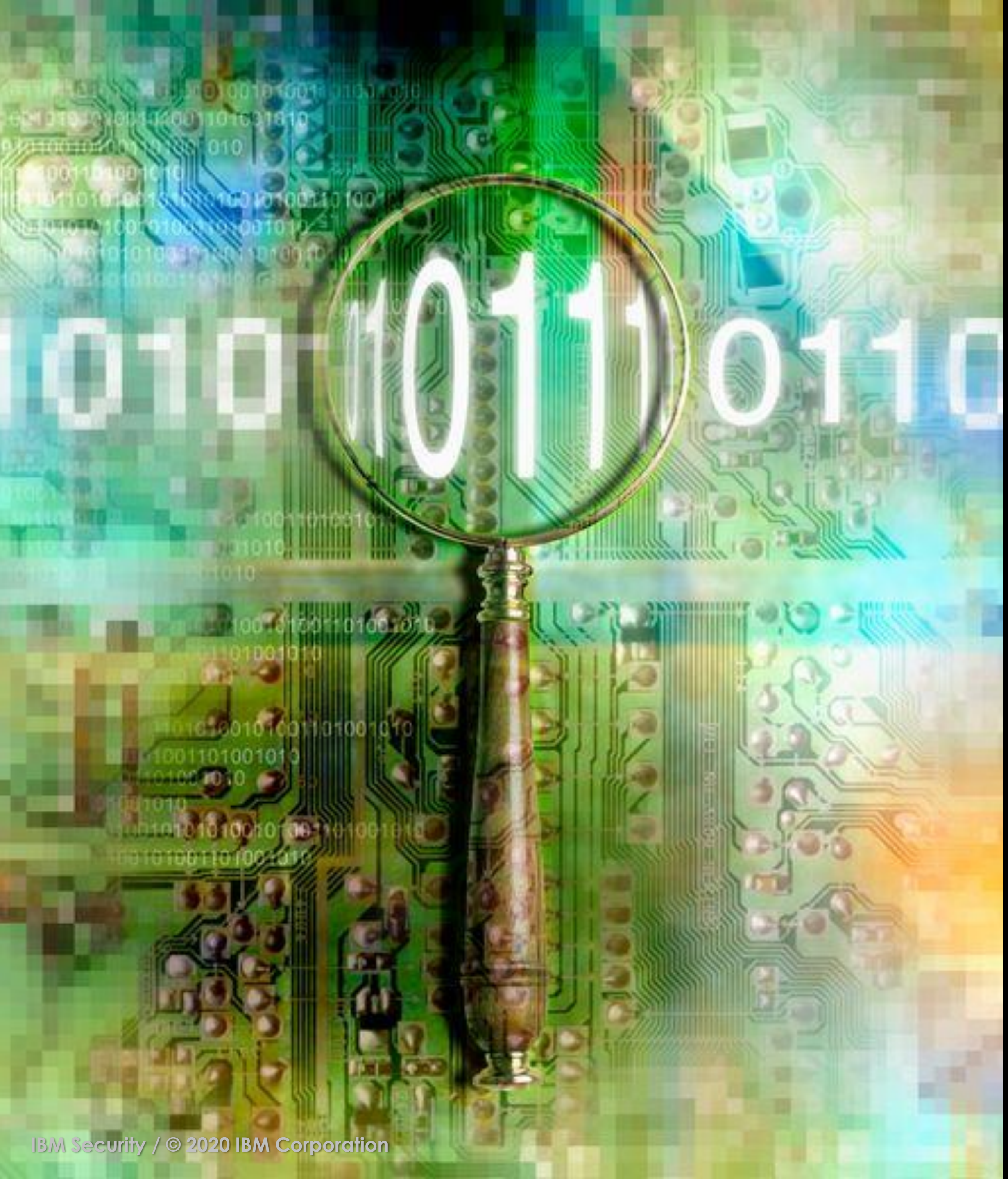


Number of organizations that said automation, machine learning, AI and orchestration increases cyber resilience



Prepare communications in advance

- ✓ Authorized Spokesperson
- ✓ Concise Content
- ✓ Internal versus External
- ✓ Communications Channels
- ✓ Update Frequency



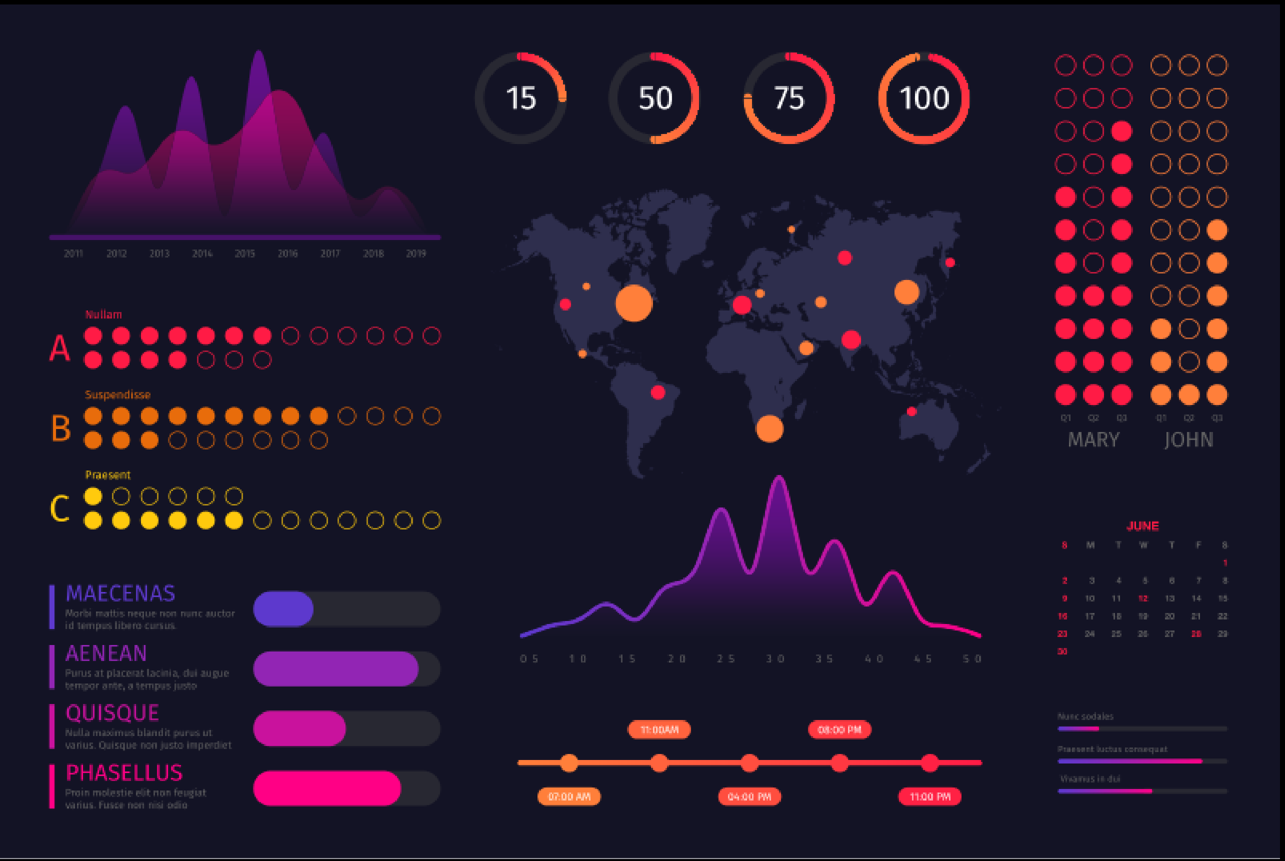
Test your plan like your business depends on it

Why Test?

Test your plan with a variety of methods

Use different scenarios to evaluate different aspects of your plan

Measure and communicate the results to the organization



Why measure?

Program metrics

Testing metrics

Provide visibility of your Cyber Resiliency metrics to executive leadership and your Board of Directors

Summary

Plan for the obvious and not so obvious threats

- Black Swans
- Gray Rhinos
- Elephants

Listen to Cassandras

Plan to be cyber resilient

- Business Continuity
- Disaster Recovery
- Incident Response

One Team with One Goal

Automate resiliency and response

- Increase use of cloud-based solutions
- Reduce complexity and number of tools

Test and measure regularly

- Test multiple scenarios using different methods
- Measure and report your outcomes for improvement

Ponemon 2020 Cyber Resilient Organization Report – LINK

Ponemon 2020 Cost of a Data Breach Report - LINK

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.